Math 116: Practice Midterm

Owen Jones

2/16/2024

1. | | x | y |
   |---|---|---|
   | 26 | 1 | 0 |
   | 17 | 0 | 1 |
   | 9 | 1 | -1 |
   | 8 | -1 | 2 |
   | 1 | 2 | -3 |

   $m = -3(E(m) - 6) \pmod{26}$
   $BANG$
   675

2. $n \mid x^3 - y^3 \Rightarrow n \mid (x-y)(x^2+xy+y^2)$.
   Let $d = \gcd(x-y, n)$. If $d = 1$ then $\exists$ integers s, t s.t $n(x^2+xy+y^2)s + nt = (x^2+xy+y^2) \Rightarrow n \mid (x^2+xy+y^2)$ which is is known to be false. If $d = n$ then $n \mid (x-y)$ which we also know to be false. Thus, d must be a non-trivial factor of n.

3. $a_0 = 2^{65} \equiv 8192 \pmod{n}$
   $a_1 = (-129)^2 \equiv -1 \pmod{n}$
   $\Rightarrow$ 8321 is probably prime.

4. Let $c \in Im(E_k)$, i.e there exists some $m \in \mathcal{P}$ s.t $c = E_k(m)$. By (1), we obtain $D_k(c) = m \Rightarrow c = E_k(m) = E_k(D_k(c))$. It suffices to show $Im(E_k) = \mathcal{C}$. E_k must be 1 to 1 for (1) to hold because D_k can't map an encrypted message to multiiple plaintext messages. Because $\mathcal{C}$ and $\mathcal{P}$ are the same size, E_k must be onto. Thus, $\mathcal{C} = Im(E_k)$.